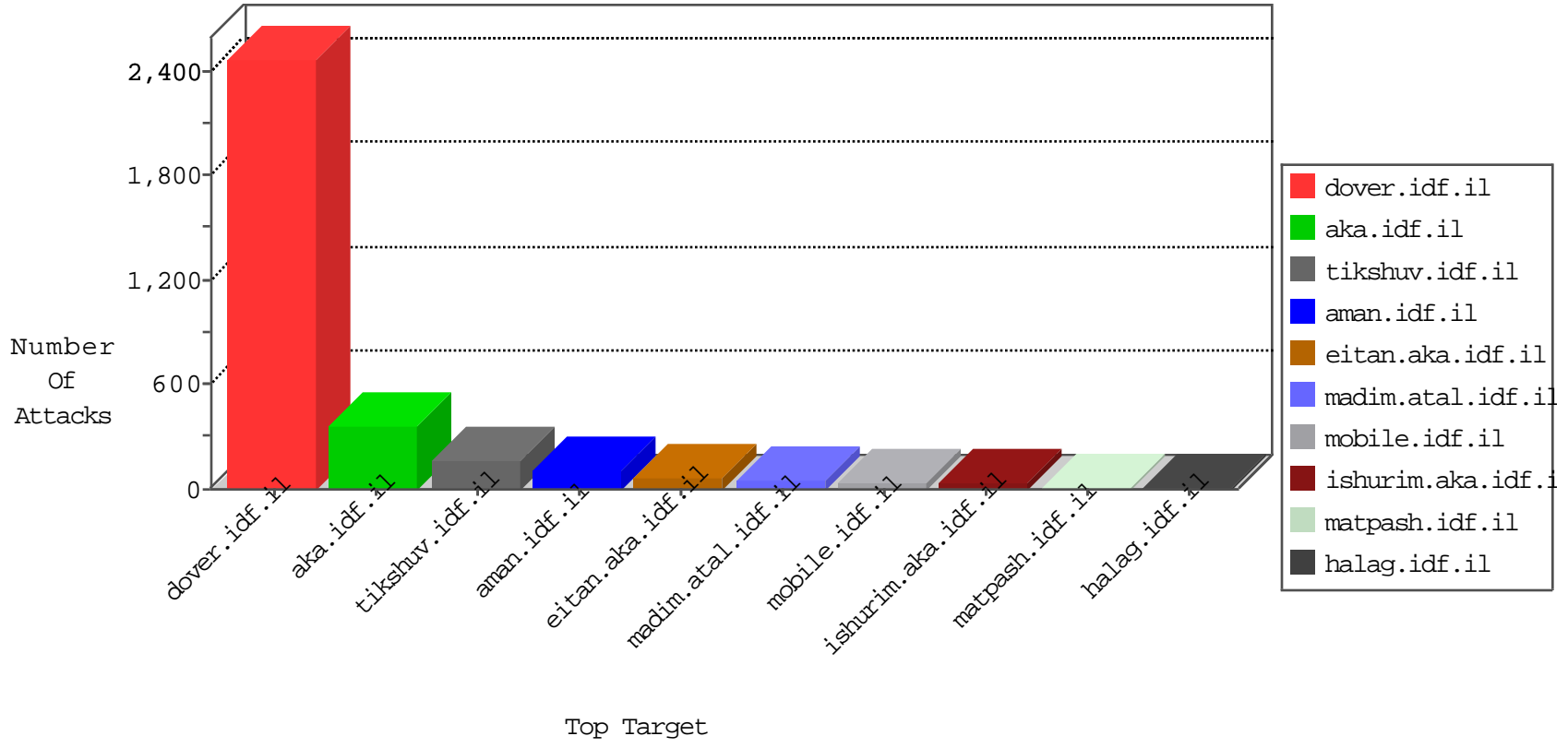


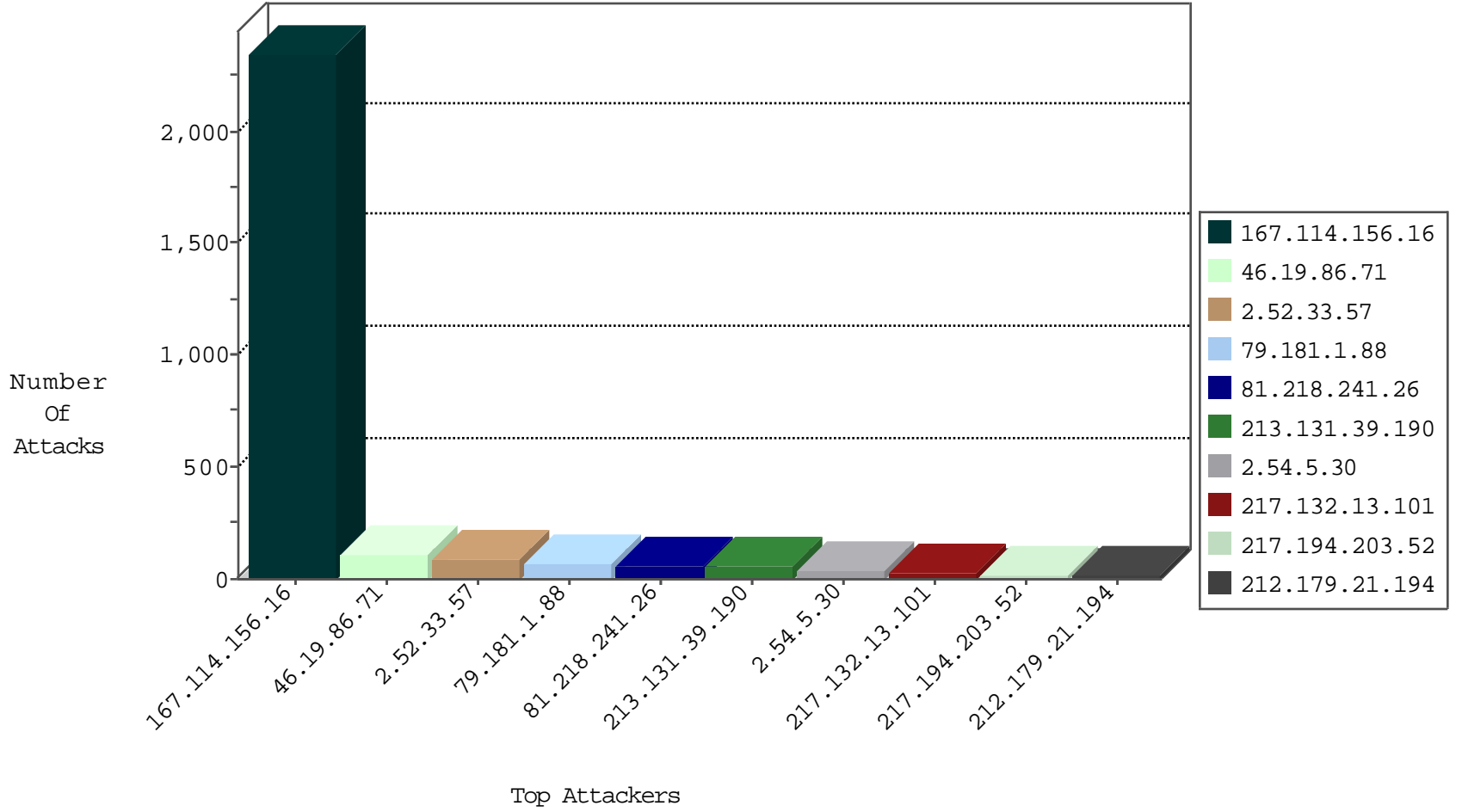
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	3576
81.218.241.26	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	104
81.218.241.26	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	102
81.218.65.210	Israel	147.237.0.34	tikshuv.idf.il	Block_Udp_All_Nets	drop	3
81.218.65.210	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
216.218.206.93	United States	147.237.77.235	sviva.idf.il	Block_Udp_All_Nets	drop	1
180.212.120.52	China	147.237.8.14	e.orchot.idf.il	Block_Udp_All_Nets	drop	1
184.105.139.118	United States	147.237.8.27	e.madim.atal.idf.il	Block_Ntp_All_Net	drop	1
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.54.32.155	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	10
149.88.89.46	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
2.54.3.159	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
2.54.157.132	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
79.183.192.171	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
176.13.12.107	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
192.115.83.5	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
159.122.222.207	Netherlands	147.237.0.17	m.my-kosher-kravi.idf.il	20085: HTTP: Mueblackcat Security Scanner Initial Request	Block	1
83.42.185.182	Spain	147.237.77.176	matpash.idf.il	C1000008: HTTP: Xenu UserAgent	Block	1

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	3
84.228.220.4	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
80.246.136.216	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
61.182.170.38	147.237.76.86	China	navy.idf.il	ET SCAN Potential SSH Scan	1
167.114.156.16	147.237.77.216	Canada	dover.idf.il	portscan: TCP Distributed Portscan	1
85.250.7.254	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
84.111.168.182	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.183.236.137	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
61.182.170.38	147.237.76.31	China	rakchal.idf.il	ET SCAN Potential SSH Scan	1
217.132.37.71	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
176.13.21.221	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
93.172.169.63	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
46.19.86.71	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	105
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	63
79.181.1.88	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	63
81.218.241.26	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	23
217.132.13.101	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	19
213.131.39.190	Georgia	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	17
2.52.33.57	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	17
2.52.33.57	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	16
2.52.33.57	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	16
2.52.33.57	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	16
213.131.39.190	Georgia	147.237.72.156	aman.idf.il	Bad TCP sequence		monitor	14
217.194.203.52	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	12
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack		reject	12
212.179.21.194	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	12
81.218.241.26	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	12
2.52.33.57	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	12
46.19.85.54	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
2.52.33.57	Israel	147.237.72.166	aka.idf.il	SYN Attack		reject	10
46.19.85.134	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
213.131.39.190	Georgia	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
213.131.39.190	Georgia	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
194.114.146.227	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
2.54.164.113	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
2.54.5.50	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
46.19.86.53	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.155.129	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.63	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.52.141.12	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
213.131.39.190	Georgia	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.67	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
109.66.105.59	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.66.115.224	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
77.125.96.189	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
62.219.120.45	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.1.181	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
185.26.180.108	United Kingdom	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
46.116.145.54	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
2.54.172.172	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
109.64.106.93	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
109.64.106.93	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
46.19.85.125	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
77.125.108.120	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
85.203.17.136	Netherlands	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
77.125.108.120	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
87.106.179.116	Germany	147.237.77.74	law.idf.il	drop	SAM rule	drop	4
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
2.54.40.171	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
141.0.15.195	Norway	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.54.5.30	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	32
147.235.8.61	Israel	147.237.77.243	mobile.idf.il	Distributed Parameter Type Violation on mobile.idf.il/sachar/changepassword parameter CurrentPassword	Block	13
176.13.20.58	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	9
192.116.232.69	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 192.116.232.69	Block	4
185.68.109.226	Spain	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 185.68.109.226	Block	3
109.253.223.5	Israel	147.237.77.243	mobile.idf.il	Distributed Parameter Type Violation on mobile.idf.il/sachar/changepassword parameter CurrentPassword	Block	3
2.54.170.130	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.15.77	Israel	147.237.77.243	mobile.idf.il	Distributed Parameter Type Violation on mobile.idf.il/sachar/changepassword parameter CurrentPassword	Block	3
109.253.223.5	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation Password in mobile.idf.il/sachar/login	Block	3
2.54.56.234	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
192.117.236.29	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/1048-7488-he/scriptresource.axd	Block	2
46.19.85.80	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
37.26.147.186	Israel	147.237.76.147	chinuch.aka.idf.il	Distributed Unauthorized URL Access on www.chinuch.aka.idf.il/404.htm	Block	2
37.26.148.149	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	1
192.116.232.69	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/images/1.he/trigger.png	Block	1
66.249.78.97	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
213.131.39.190	Georgia	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	1
5.22.129.246	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files	Block	1
109.64.176.204	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/undefined	Block	1
37.26.148.241	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	1
147.235.8.61	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation NewPassword in mobile.idf.il/sachar/changepassword	Block	1
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
216.218.206.66	United States	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to 147.237.0.19/	Block	1
27.159.192.115	China	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	1
185.68.109.226	Spain	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/test/wp-admin/	Block	1
109.65.251.56	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
2.54.157.132	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
195.154.207.160	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/homepage/shared/usercontrols/headerupper/	Block	1
157.55.39.59	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
67.183.215.221	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
31.210.178.215	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
192.115.130.253	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/valtam	Block	1
46.19.85.80	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/nekudot/index	Block	1
197.7.172.18	Tunisia	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
79.176.86.123	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/templatecontrols/generic/	Block	1
2.52.141.12	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
46.121.120.195	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00\$ctl00\$cphMain\$TochenPlaceHolder\$btnAtudaBack in www.aka.idf.il/main/giyus/atuda/asmachta.aspx	None	1
207.46.13.123	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atall/izkor/print_bottom.asp	Block	1
5.22.129.246	Israel	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 5.22.129.246	Block	1
79.177.125.14	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/home/default.aspx	Block	1